PATENT
B588-042

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Satoru Wakao, Akira Akashi
Serial No.	:	10/797,827
Filed	:	March 10, 2004
For	:	DIGITAL SIGNATURE GENERATING APPARATUS, METHOD, COMPUTER PROGRAM AND COMPUTER-READABLE STORAGE MEDIUM
Examiner	:	Unassigned
Art Unit	:	2131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

CLAIM TO BENEFIT OF 35 U.S.C. § 119
AND FILING OF PRIORITY DOCUMENT

Claim is made herein to the benefit of 35 U.S.C. § 119 of the filing date of the following Japanese Patent Application: 2003-071033 (filed March 14, 2003) a certified copy of which are filed herewith.

Dated: August 17, 2004

Respectfully submitted,

John J. Torrente

COWAN, LIEBOWITZ & LATMAN, P.C.
1133 Avenue of the Americas
New York, NY 10036-6799
(212) 790-92000

John J. Torrente
Registration No. 26,359
An Attorney of Record

25815/000/642247.1

CFM0350
U
C

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月１４日

出願番号
Application Number: 特願２００３－０７１０３３

[ST. 10/C]: ［ＪＰ２００３－０７１０３３］

出願人
Applicant(s): キヤノン株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００４年　３月２９日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　253927
【提出日】　平成15年 3月14日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明の名称】　デジタル署名生成装置、方法、コンピュータプログラム、およびコンピュータ読み取り可能な記憶媒体
【請求項の数】　12
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　若尾　聡
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　明石　彰
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100090273
【弁理士】
【氏名又は名称】　國分　孝悦
【電話番号】　03-3590-8901
【手数料の表示】
【予納台帳番号】　035493
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705348

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　デジタル署名生成装置、方法、コンピュータプログラム、およびコンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項１】　複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置であって、

鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更し、

署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成することを特徴とするデジタル署名生成装置。

【請求項２】　前記デジタル署名生成装置は、ＩＣカードであることを特徴とする請求項１に記載のデジタル署名生成装置。

【請求項３】　前記デジタル署名生成装置は、マルチアプリケーションＯＳを搭載した装置であることを特徴とする請求項２に記載のデジタル署名生成装置。

【請求項４】　前記鍵変更コマンドは、前記複数の秘密鍵の何れか一つを指定する情報を含むコマンドであることを特徴とする請求項１～３のいずれか１項に記載のデジタル署名生成装置。

【請求項５】　署名生成コマンドは、前記デジタルデータのハッシュ値を含むコマンドであることを特徴とする請求項１～４のいずれか１項に記載のデジタル署名生成装置。

【請求項６】　複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置におけるデジタル署名生成方法であって、

鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更する工程と、

署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成する工程とを有することを特徴とするデジタル署名生成方法。

【請求項７】　前記デジタル署名生成装置は、ＩＣカードであることを特徴とする請求項６に記載のデジタル署名生成方法。

【請求項８】　前記デジタル署名生成装置は、マルチアプリケーションＯＳを搭載した装置であることを特徴とする請求項７に記載のデジタル署名生成方法。

【請求項９】　前記鍵変更コマンドは、前記複数の秘密鍵の何れか一つを指定する情報を含むコマンドであることを特徴とする請求項６～８のいずれか１項に記載のデジタル署名生成方法。

【請求項１０】　署名生成コマンドは、前記デジタルデータのハッシュ値を含むコマンドであることを特徴とする請求項６～９のいずれか１項に記載のデジタル署名生成方法。

【請求項１１】　請求項６～１０のいずれか１項に記載のデジタル署名生成方法の各工程をコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項１２】　請求項１１に記載のコンピュータプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルデータ（画像データなど）のデジタル署名を生成するデジタル署名生成装置、方法、コンピュータプログラム、およびコンピュータ読み取り可能な記憶媒体に関するものである。

【０００２】

【従来の技術】

現在、デジタルカメラなどの撮像装置で撮像されたオリジナル画像データのデジタル署名をＩＣカード内で生成するシステムが提案されている（例えば、特許文献１）。

【０００３】

【特許文献１】

特開２００２－２４４９２４号公報

【０００４】

【発明が解決しようとする課題】

しかしながら、従来のＩＣカードは、デジタル署名用の秘密鍵を一つしか備えていなかった。そのため、特別なユーザに通常のユーザとは異なる秘密鍵を提供する場合、特別なユーザ用の秘密鍵を有するＩＣカードを製造し直さなければならず、特別なユーザ用のＩＣカードの製造コストが上昇してしまうという問題があった。

【０００５】

本発明は、このような問題に鑑みてなされたものであり、製造コストを高めることなく、特別なユーザに通常のユーザとは異なるデジタル署名用の鍵情報を提供できるようにすることを目的とする。

【０００６】

【課題を解決するための手段】

本発明におけるデジタル署名生成装置は、複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置であって、鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更し、署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成することを特徴とする。

【０００７】

本発明におけるデジタル署名生成方法は、複数の秘密鍵を記憶した記憶手段とを有するデジタル署名生成装置におけるデジタル署名生成方法であって、鍵変更コマンドを受信した場合には、前記デジタル署名生成装置が使用する秘密鍵を前記鍵変更コマンドが指定する秘密鍵に変更する工程と、署名生成コマンドを受信した場合には、前記複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成する工程とを有することを特徴とする。

【０００８】

【発明の実施の形態】

以下、図面を参照し、本発明に好適な実施の形態を説明する。

［第１の実施の形態］

まず、図１を参照し、第１の実施の形態におけるデジタル署名生成システムの主要な構成要素を説明する。

【０００９】

ＩＣカード１０は、マルチアプリケーションＯＳ(Operating System)を搭載したＩＣカードであり、複数のアプリケーションプログラムの実行が可能なＩＣカードである。ＩＣカード１０は、複数の秘密鍵を記憶した記憶媒体を有し、複数の秘密鍵の何れか一つを用いてデジタルデータＭ（画像データなど）のデジタル署名Ｓを生成することができる。ＩＣカード１０は、接触型であっても、非接触型であっても、ハイブリッド型（接触型および非接触型の機能を有する）であってもよい。なお、ＩＣカード１０は、デジタルデータＭのデジタル署名Ｓを生成する装置であるので、「デジタル署名生成装置」と呼ぶこともできる。

【００１０】

コンピュータＡ２０は、ベンダーが使用するコンピュータである。記録媒体Ａ２１は、コンピュータＡ２０にインストールされるプログラムＡを記録した記録媒体である。プログラムＡは、コンピュータＡ２０での実行が可能なプログラムであり、秘密鍵変更処理（図５参照）および秘密鍵確認処理（図６参照）の実行に必要なプログラムである。

【００１１】

コンピュータＢ３０は、通常又は特別なユーザが使用するコンピュータである。記録媒体Ｂ３１は、コンピュータＢ３０にインストールされるプログラムＢを記録した記録媒体である。プログラムＢは、コンピュータＢ３０での実行が可能なプログラムであり、デジタル署名生成処理（図７参照）の実行に必要なプログラムである。

【００１２】

次に、図２を参照し、本実施の形態におけるＩＣカード１０の主要な構成要素を説明する。インターフェースユニット１０１は、コンピュータＡ２０又はコンピュータＢ３０から送信されたコマンドを受信し、受信したコマンドに対応するレスポンスをコンピュータＡ２０又はコンピュータＢ３０に送信するユニットで

ある。

【００１３】

ＣＰＵ（Central Processing Unit）１０２は、ＥＥＰＲＯＭ１０４が記憶する複数のアプリケーションプログラムに従ってＩＣカード１０の動作を制御するユニットである。

【００１４】

ＲＯＭ（Read Only Memory）１０３は、マルチアプリケーションＯＳ、コマンドインタープリタを記憶するメモリである。マルチアプリケーションＯＳは、ＥＥＰＲＯＭ１０４が記憶する複数のアプリケーションプログラムを管理するオペレーティングシステムである。マルチアプリケーションＯＳには、入出力機能、暗号機能、ファイル管理機能、ＥＥＰＲＯＭ１０４に新しいアプリケーションプログラムを追加する機能、ＥＥＰＲＯＭ１０４が記憶するアプリケーションプログラムを削除する機能などがある。

【００１５】

ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）１０４は、複数の秘密鍵を管理する鍵管理テーブル、複数のアプリケーションプログラム、ユーザデータなどを記憶するメモリである。

【００１６】

ＲＡＭ（Random Access Memory）１０５は、ＣＰＵ１０２およびコプロセッサ１０６が扱うデータを一時的に記憶するメモリである。

【００１７】

コプロセッサ（Co-Processor）１０６は、ＥＥＰＲＯＭ１０４が記憶する複数の秘密鍵の一つを用いてデジタルデータＭのハッシュ値を暗号化することによってデジタルデータＭのデジタル署名Ｓを生成するユニットである。暗号化アルゴリズムには、ＲＳＡ暗号などの公開鍵暗号を利用する。

【００１８】

次に、図３を参照し、ＩＣカード１０のＥＥＰＲＯＭ１０４が記憶する鍵管理テーブルの一例を説明する。鍵管理テーブルは、ＩＣカード１０が使用する秘密鍵を管理する管理テーブルである。鍵管理テーブルには、図３に示すように、複

数個の秘密鍵（本実施の形態では１６個）が登録されている。０番の秘密鍵は通常のユーザ用の秘密鍵である。製造直後のＩＣカード１０の秘密鍵は０番の秘密鍵に設定されている。１番～１５番までの秘密鍵は特別なユーザ用の秘密鍵である。ある特別なユーザに３番の秘密鍵を提供する場合、ベンダーはコンピュータＡ２０を使用してＩＣカード１０に鍵変更コマンド（３番の秘密鍵を指定）を送信する。鍵変更コマンドの実行が正常に終了すれば、ＩＣカード１０の秘密鍵は３番の秘密鍵となり、特別なユーザに通常のユーザとは異なる秘密鍵を提供することができる。

【００１９】

次に、図４を参照し、コンピュータＡ２０又はコンピュータＢ３０からＩＣカード１０に送信されるコマンドのデータフォーマット、および、ＩＣカード１０からコンピュータＡ２０又はコンピュータＢ３０に送信されるレスポンスのデータフォーマットを説明する。

【００２０】

コマンド識別コードフィールド４０１は、コマンドの種別を表すコマンド識別コードを格納するフィールドである。コマンドには、鍵変更コマンド、鍵確認コマンド、署名生成コマンドなどがある。鍵変更コマンドは、ＩＣカード１０が使用する秘密鍵をベンダーによって選択された秘密鍵に変更することをＩＣカード１０に要求するコマンドである。鍵確認コマンドは、ＩＣカード１０に設定されている秘密鍵の鍵番号をＩＣカード１０に問い合せるコマンドである。署名生成コマンドは、ユーザによって選択されたデジタルデータＭのデジタル署名Ｓを生成することをＩＣカード１０に要求するコマンドである。

【００２１】

コマンドデータ長フィールド４０２は、コマンドデータフィールド４０３のデータ長（バイト長）を格納するフィールドである。

【００２２】

コマンドデータフィールド４０３は、ＩＣカード１０に送信するデータを格納するフィールドである。鍵変更コマンドの場合、コマンドデータフィールド４０３にはＩＣカード１０に設定したい秘密鍵の鍵番号が格納される。鍵確認コマン

ドの場合、コマンドデータフィールド４０３には何も格納されない。署名生成コマンドの場合、コマンドデータフィールド４０３にはデジタルデータＭ（画像データなど）が格納される。

【００２３】

レスポンスデータ長フィールド４０４は、レスポンスデータフィールド４０５のデータ長（バイト長）を格納するフィールドである。

【００２４】

レスポンスデータフィールド４０５は、コマンドに対応するデータを格納するフィールドである。鍵変更コマンドの実行が正常に終了した場合、レスポンスデータフィールド４０５には鍵変更コマンドに従って設定された秘密鍵の鍵番号が格納される。鍵確認コマンドの実行が正常に終了した場合、レスポンスデータフィールド４０５にはＩＣカード１０に設定されている秘密鍵の鍵番号が格納される。署名生成コマンドの実行が正常に終了した場合、署名生成コマンドから取り出されたデジタルデータのデジタル署名が格納される。鍵変更コマンド、鍵確認コマンド又は署名生成コマンドの実行が正常に終了しなかった場合、レスポンスデータフィールド４０５にはダミーデータが格納される。

【００２５】

状態コードフィールド４０６は、コマンドを実行した結果（正常終了、エラー、警告など）を表す状態コードを格納するフィールドである。

【００２６】

次に、図５を参照し、コンピュータＡ２０とＩＣカード１０との間で実行される秘密鍵変更処理の手順を説明する。秘密鍵変更処理は、ＩＣカード１０が使用する秘密鍵をベンダーが選択した秘密鍵に変更する処理である。秘密鍵変更処理は、ＩＣカード１０の製造後、ベンダー側で行われる処理である。

【００２７】

ステップＳ５０１：コンピュータＡ２０は、ベンダーの指示に従って鍵変更コマンドを生成し、生成した鍵変更コマンドをＩＣカード１０に送信する。このとき、鍵変更コマンドのコマンドデータフィールド４０３には、ベンダーによって選択された鍵番号が格納されている。

【００２８】

ステップＳ５０２：インターフェースユニット１０１は、鍵変更コマンドを受信し、受信した鍵変更コマンドをＣＰＵ１０２に供給する。ＣＰＵ１０２は、鍵変更コマンドのコマンドデータフィールド４０３から鍵番号を取り出し、取り出した鍵番号を有効にするべく鍵管理テーブルを更新する。つまり、鍵変更コマンドが指定する秘密鍵をＩＣカード１０が使用する秘密鍵に変更する。例えば、鍵変更コマンドが指定する鍵番号が３番である場合、ＩＣカード１０が使用する秘密鍵は３番の秘密鍵に変更される。

【００２９】

ステップＳ５０３：ＣＰＵ１０２は、鍵変更コマンドを実行した結果からレスポンスを生成し、生成したレスポンスをインターフェースユニット１０１に供給する。このとき、レスポンスのレスポンスデータフィールド４０５には、変更後の鍵番号が格納されている。インターフェースユニット１０１は、レスポンスをコンピュータＡ２０に返信する。

【００３０】

ステップＳ５０４：コンピュータＡ２０は、レスポンスを受信し、受信したレスポンスを解析する。鍵変更コマンドが正常に終了した場合、コンピュータＡ２０は、変更後の鍵番号をベンダーに通知する。これにより、ベンダーは、ＩＣカード１０に設定されたデジタル署名用の秘密鍵を知ることができる。鍵変更コマンドが正常に終了しなかった場合、コンピュータＡ２０は、状態コードを用いて鍵変更コマンドが正常に終了しなかった理由をベンダーに通知する。

【００３１】

次に、図６を参照し、コンピュータＡ２０とＩＣカード１０との間で実行される秘密鍵確認処理の手順を説明する。秘密鍵確認処理は、ＩＣカード１０が使用するデジタル署名用の秘密鍵を確認する処理である。秘密鍵確認処理は、ベンダー側で行われる処理である。

【００３２】

ステップＳ６０１：コンピュータＡ２０は、ベンダーの指示に従って鍵確認コマンドを生成し、生成した鍵確認コマンドをＩＣカード１０に送信する。このと

き、鍵確認コマンドのコマンドデータフィールド４０３には、何も格納されていない。

【００３３】

ステップＳ６０２：インターフェースユニット１０１は、鍵確認コマンドを受信し、受信した鍵確認コマンドをＣＰＵ１０２に供給する。ＣＰＵ１０２は、インターフェースユニット１０１から供給された鍵確認コマンドを実行する。ＣＰＵ１０２は、鍵管理テーブルを参照し、ＩＣカード１０に設定されている鍵番号を調べる。

【００３４】

ステップＳ６０３：ＣＰＵ１０２は、鍵確認コマンドを実行した結果からレスポンスを生成し、生成したレスポンスをインターフェースユニット１０１に供給する。このとき、レスポンスのレスポンスデータフィールド４０５には、ＩＣカード１０に設定されている鍵番号が格納されている。インターフェースユニット１０１は、レスポンスをコンピュータＡ２０に返信する。

【００３５】

ステップＳ６０４：コンピュータＡ２０は、レスポンスを受信し、受信したレスポンスを解析する。鍵確認コマンドが正常に終了した場合、コンピュータＡ２０は、ＩＣカード１０に設定されている鍵番号をベンダーに通知する。これにより、ベンダーは、ＩＣカード１０に設定されているデジタル署名用の秘密鍵を知ることができる。鍵確認コマンドが正常に終了しなかった場合、コンピュータＡ２０は、状態コードを用いて鍵確認コマンドが正常に終了しなかった理由をベンダーに通知する。

【００３６】

次に、図７を参照し、コンピュータＢ３０とＩＣカード１０との間で実行されるデジタル署名生成処理の手順を説明する。デジタル署名生成処理は、ＩＣカード１０に設定されているデジタル署名用の秘密鍵を用いてデジタルデータＭのデジタル署名Ｓを生成する処理である。デジタル署名生成処理は、通常又は特別なユーザ側で行われる処理である。

【００３７】

ステップＳ７０１：コンピュータＢ３０は、通常又は特別なユーザの指示に従って署名生成コマンドを生成し、生成した署名生成コマンドをＩＣカード１０に送信する。このとき、署名生成コマンドのコマンドデータフィールド４０３には、デジタルデータMが格納されている。

【００３８】

ステップＳ７０２：インターフェースユニット１０１は、署名生成コマンドを受信し、受信した署名生成コマンドをＣＰＵ１０２に供給する。ＣＰＵ１０２は、鍵変更コマンドのコマンドデータフィールド４０３からデジタルデータMを取り出し、取り出したデジタルデータMをＲＡＭ１０５に書き込む。ＣＰＵ１０２は、鍵管理テーブルからＩＣカード１０に設定されている秘密鍵を取り出し、取り出した秘密鍵をＲＡＭ１０５に書き込む。コンピュータＢ３０のユーザが通常のユーザである場合、ＣＰＵ１０２は、０番の秘密鍵をＲＡＭ１０５に書き込む。コンピュータＢ３０のユーザが特別なユーザである場合、コプロセッサ１０６は、１番から１５番の何れかの秘密鍵をＲＡＭ１０５に書き込む。コプロセッサ１０６は、デジタルデータMのデジタル署名Ｓを生成するために、ＲＡＭ１０５から読み出したデジタルデータMからデジタルデータMのハッシュ値を生成し、生成したハッシュ値をＲＡＭ１０５から読み出した秘密鍵によって暗号化する。コプロセッサ１０６は、生成したデジタル署名ＳをＲＡＭ１０５に書き込む。

【００３９】

ステップＳ７０３：ＣＰＵ１０２は、署名生成コマンドを実行した結果からレスポンスを生成し、生成したレスポンスをインターフェースユニット１０１に供給する。署名生成コマンドの実行が正常に終了した場合、レスポンスデータフィールド４０５にはＲＡＭ１０５から読み出されたデジタル署名Ｓが格納される。署名生成コマンドの実行が正常に終了しなかった場合、レスポンスデータフィールド４０５にはダミーデータが格納される。インターフェースユニット１０１は、レスポンスをコンピュータＢ３０に返信する。

【００４０】

ステップＳ７０４：コンピュータＢ３０は、レスポンスを受信し、受信したレスポンスを解析する。署名生成コマンドの実行が正常に終了した場合、コンピュ

ータＢ３０は、デジタル署名Ｓが正常に生成されたことをユーザに通知する。そして、コンピュータＢ３０は、レスポンスデータフィールド４０５からデジタル署名Ｓを取り出し、取り出したデジタル署名ＳをデジタルデータＭに付加する。署名生成コマンドの実行が正常に終了しなかった場合、コンピュータＢ３０は、正常に終了しなかった理由をユーザに通知する。

【００４１】

次に、図８を参照し、特別なユーザ用の秘密鍵を設定したＩＣカード１０を特別なユーザに提供する手順を説明する。

【００４２】

ステップＳ８０１：ベンダーは、特別なユーザからＩＣカード１０を受け取る。

【００４３】

ステップＳ８０２：ベンダーは、特別なユーザに使用させる鍵番号（１番から１５番までの何れか）を決定する。

【００４４】

ステップＳ８０３：ベンダーは、ステップＳ８０２で決定した鍵番号をＩＣカード１０に設定する。鍵番号の設定には、上記の鍵変更コマンドを使用する。この処理により、ＩＣカード１０には通常のユーザとは異なる秘密鍵が設定される（通常のユーザの鍵番号は０番である）。例えば、ステップＳ８０２で決定した鍵番号が３番である場合、ＩＣカード１０の秘密鍵は３番に対応する秘密鍵となる。

【００４５】

ステップＳ８０４：ベンダーは、ＩＣカード１０を特別なユーザに提供する。これにより、ベンダーは、特別なユーザに通常のユーザとは異なるデジタル署名用の秘密鍵を提供することができる。

【００４６】

このように、第１の実施の形態におけるＩＣカード１０によれば、鍵変更コマンドによって使用する秘密鍵を変更することができるので、ＩＣカード１０の製造コストを高めることなく、特別のユーザに通常のユーザとは異なるデジタル署

名用の秘密鍵を提供することができる。また、特別なユーザ用の秘密鍵を複数個記憶することもできるので、特別なユーザが複数存在する場合であっても、それぞれに通常のユーザとは異なるデジタル署名用の秘密鍵を提供することもできる。

【００４７】

また、第１の実施の形態におけるＩＣカード１０によれば、マルチファンクションＯＳを搭載しているので、新しいアプリケーションプログラムの追加を容易にすることができる。つまり、デジタル署名の生成アルゴリズムを新しくすることも、上記の鍵管理テーブルを更新することも、全く新しい機能を追加することも容易にできるようになる。

【００４８】

［第２の実施の形態］

上記のデジタル署名生成処理では、署名生成コマンドのコマンドデータフィールドにデジタルデータＭを格納したが、デジタルデータＭをデジタルデータＭのハッシュ値に置き換えることも可能である。この場合、ＩＣカード１０内でデジタルデータＭのハッシュ値を生成しなくてもよくなるため、ＩＣカード１０にかかる負荷を軽減することができ、デジタル署名Ｓを高速に生成することができるようになる。またこの場合、ＩＣカード１０で扱うデータサイズを小さくすることができるので（なぜなら、デジタルデータＭのハッシュ値のデータサイズはデジタルデータＭのデータサイズよりも十分に小さいため）、ＩＣカード１０の回路規模を小さくでき、ＩＣカード１０の製造コストをより安くすることができる。

【００４９】

［第３の実施の形態］

上記のコンピュータＢ３０は、デジタルカメラ、デジタルビデオカメラ、スキャナなどの撮像装置に置き換えることも可能である。第２の実施の形態におけるデジタル署名生成システムの主要な構成要素を図９に示す。撮像装置４０は、被写体の画像データを撮像する撮像ユニットを有する装置であり、例えば、デジタルカメラ、デジタルビデオカメラ、スキャナである。記録媒体４１は、上記のデ

ジタル署名生成処理の実行に必要なプログラムを記録した記録媒体である。この場合、撮像装置４０で撮像されたオリジナル画像データのデジタル署名をＩＣカード１０で生成することが可能になる。

【００５０】

[その他の実施の形態]

上述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置或いはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステム或いは装置のコンピュータ（ＣＰＵ或いはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００５１】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体は本発明を構成する。そのプログラムコードの伝送媒体としては、プログラム情報を搬送波として伝搬させて供給するためのコンピュータネットワーク（ＬＡＮ、インターネット等のＷＡＮ、無線通信ネットワーク等）システムにおける通信媒体（光ファイバ等の有線回線や無線回線等）を用いることができる。

【００５２】

さらに、上記プログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００５３】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にも

かかるプログラムコードは本発明の実施の形態に含まれることはいうまでもない。

【００５４】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることはいうまでもない。

【００５５】

なお、上記実施の形態において示した各部の形状および構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００５６】

【発明の効果】

以上説明したように本発明によれば、製造コストを高めることなく、特別なユーザに通常のユーザとは異なるデジタル署名用の秘密鍵を提供することができる。

【図面の簡単な説明】

【図１】

第１の実施の形態におけるデジタル署名生成システムの主要な構成要素を示す図である。

【図２】

ＩＣカード１０の主要な構成要素を示す図である。

【図３】

鍵管理テーブルの一例を示す図である。

【図４】

コマンドおよびレスポンスのデータフォーマットを示す図である。

【図５】

秘密鍵変更処理の手順を説明する図である。

【図６】

秘密鍵変更処理の手順を説明する図である。

【図７】

デジタル署名生成処理の手順を説明する図である。

【図８】

特別なユーザ用の秘密鍵を設定したＩＣカード１０を特別なユーザに提供する手順を説明する図である。

【図９】

第３の実施の形態におけるデジタル署名生成システムの主要な構成要素を示す図である。

【符号の説明】

１０　ＩＣカード

２０　コンピュータＡ

２１　記録媒体Ａ

３０　コンピュータＢ

３１　記録媒体Ｂ

１０１　インターフェースユニット

１０２　ＣＰＵ

１０３　ＲＯＭ

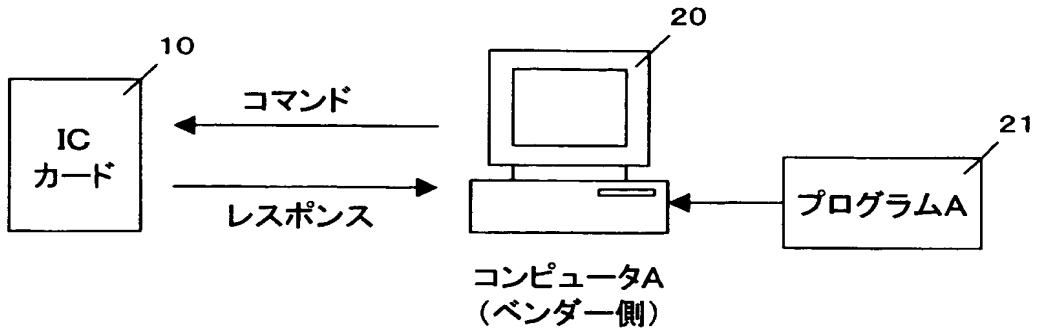
１０４　ＥＥＰＲＯＭ

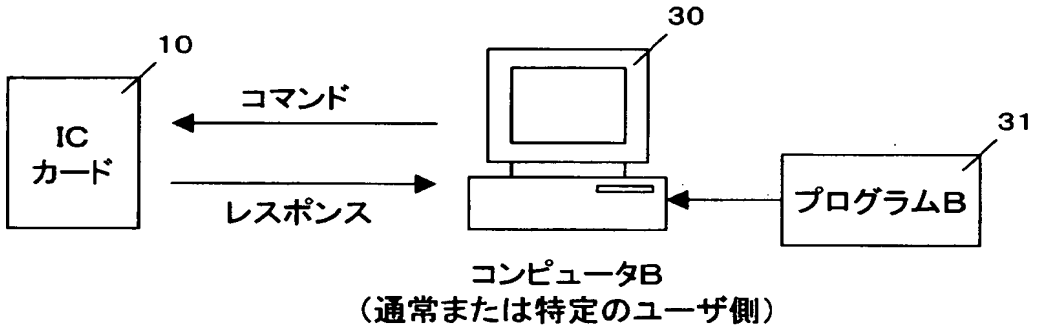
１０５　ＲＡＭ

１０６　コプロセッサ

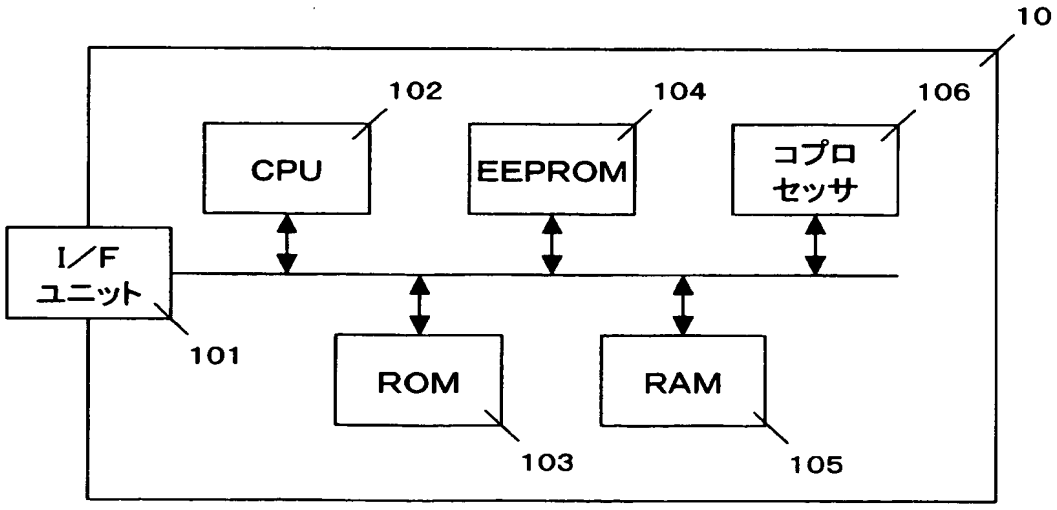
【書類名】　図面

【図１】


10
IC
カード
コマンド
レスポンス
20
21
プログラムA
コンピュータA
（ベンダー側）


10
IC
カード
コマンド
レスポンス
30
31
プログラムB
コンピュータB
（通常または特定のユーザ側）

【図２】


10
102
104
106
CPU
EEPROM
コプロ
セッサ
I/F
ユニット
101
ROM
RAM
103
105

【図３】

フラグ	鍵番号	秘密鍵
ON	0	0x9876543210AB...
OFF	1	0x876543210ABC...
OFF	2	0x76543210ABCD...
:	:	:
OFF	15	0xF9876543210A...

通常のユーザ用の秘密鍵

特定のユーザ用の秘密鍵

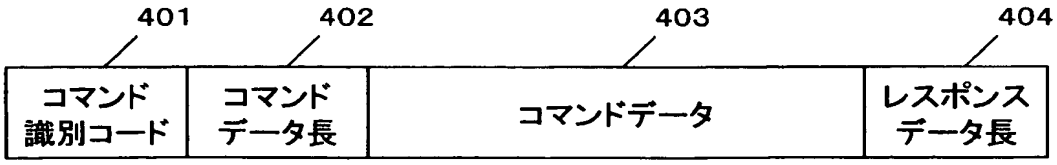
鍵設定コマンド（鍵番号3を指定）を実行した後

フラグ	鍵番号	秘密鍵
OFF	0	0x9876543210AB...
OFF	2	0x876543210ABC...
ON	3	0x76543210ABCD...
:	:	:
OFF	15	0xF9876543210A...

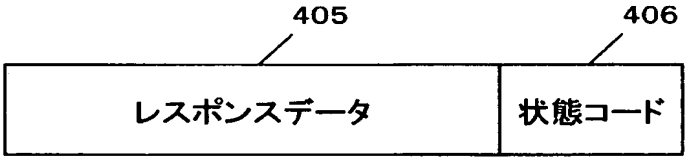
通常のユーザ用の秘密鍵

特定のユーザ用の秘密鍵

【図４】

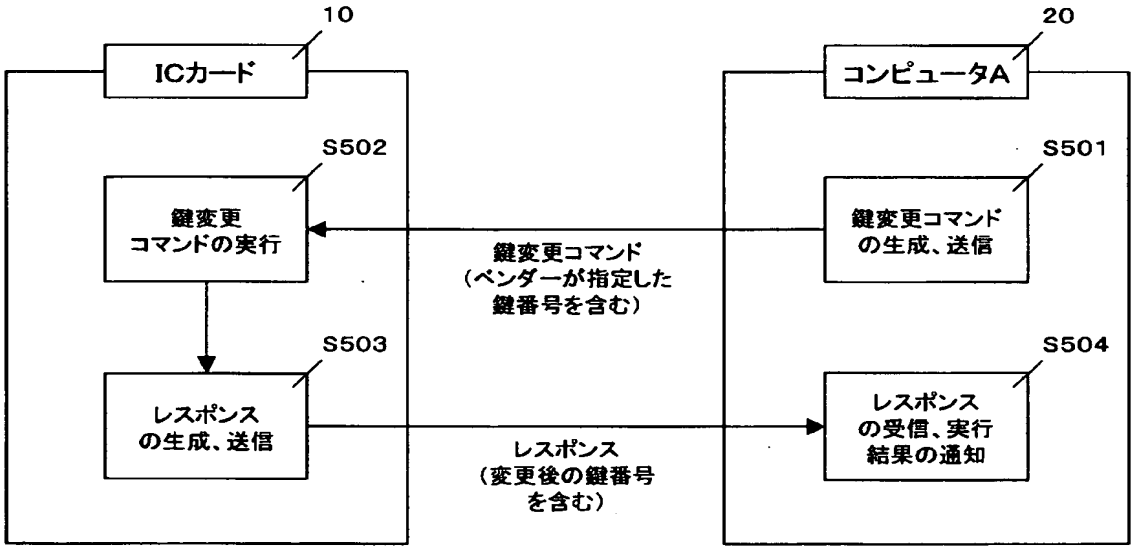


(a)コマンドのデータフォーマット

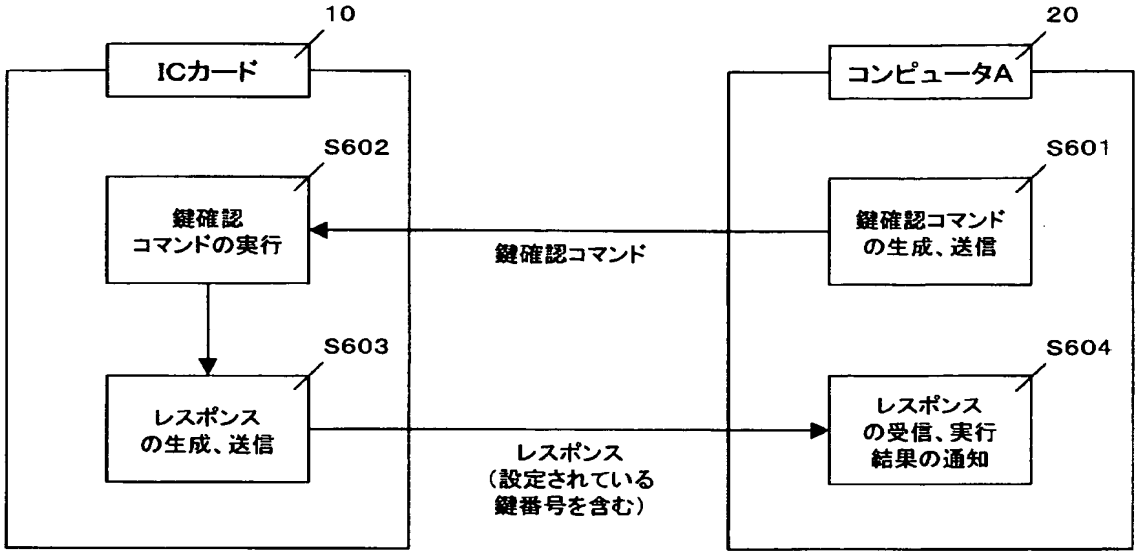


(b)レスポンスのデータフォーマット

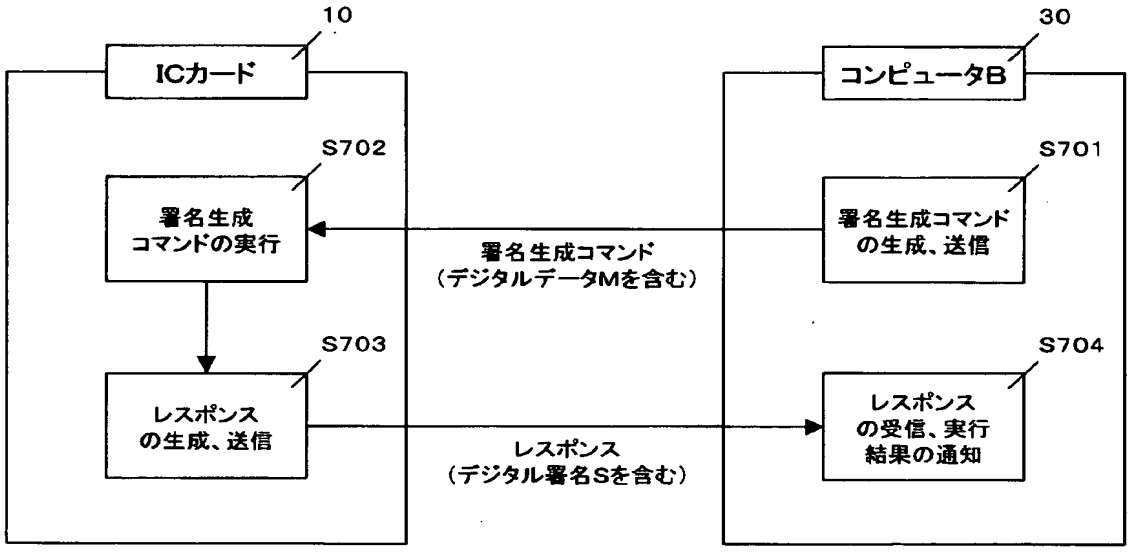
【図５】



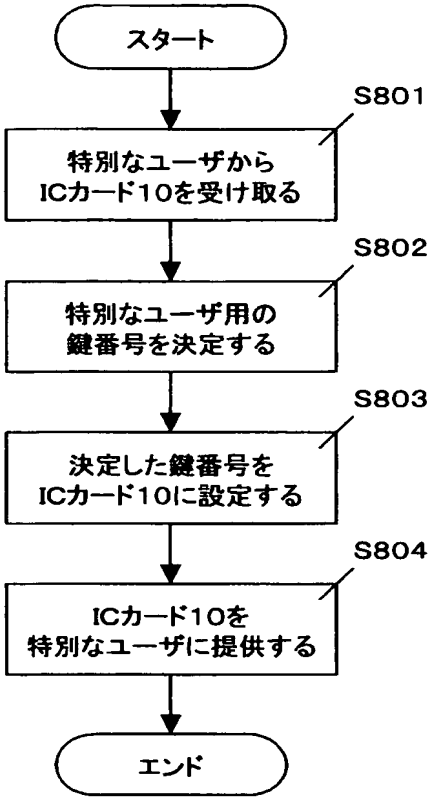
【図６】


10
ICカード
20
コンピュータA
S602
鍵確認
コマンドの実行
S601
鍵確認コマンド
の生成、送信
鍵確認コマンド
S603
レスポンス
の生成、送信
S604
レスポンス
の受信、実行
結果の通知
レスポンス
（設定されている
鍵番号を含む）

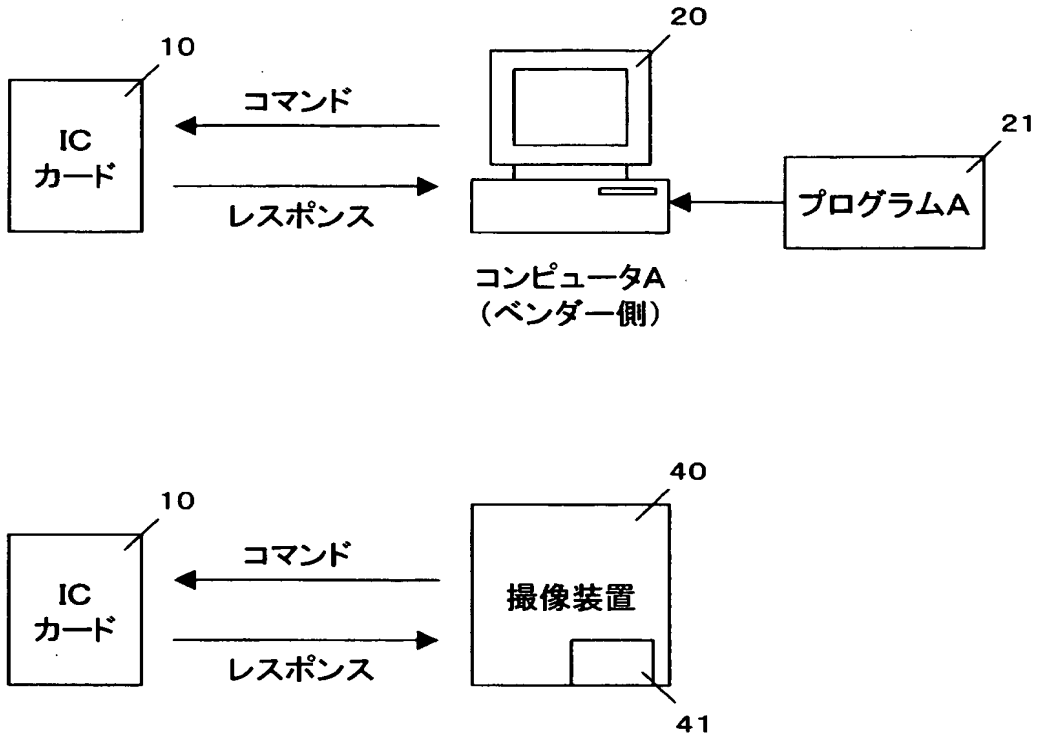
【図７】


10
ICカード
30
コンピュータB
S702
署名生成
コマンドの実行
S701
署名生成コマンド
の生成、送信
署名生成コマンド
（デジタルデータMを含む）
S703
レスポンス
の生成、送信
S704
レスポンス
の受信、実行
結果の通知
レスポンス
（デジタル署名Sを含む）

【図８】


スタート
S801
特別なユーザから
ICカード10を受け取る
S802
特別なユーザ用の
鍵番号を決定する
S803
決定した鍵番号を
ICカード10に設定する
S804
ICカード10を
特別なユーザに提供する
エンド

【図９】


10
IC
カード
コマンド
レスポンス
20
21
プログラムA
コンピュータA
（ベンダー側）
10
IC
カード
コマンド
レスポンス
40
撮像装置
41

【書類名】　　要約書

【要約】

【課題】　製造コストを高めることなく、特別なユーザに通常のユーザとは異なるデジタル署名用の秘密鍵を提供できるようにする。

【解決手段】　複数のデジタル署名用の秘密鍵を記憶するＥＥＰＲＯＭ１０４と、複数の秘密鍵の何れか一つを用いてデジタルデータのデジタル署名を生成するコプロセッサ１０６とを有し、鍵変更コマンドを受信した場合には、ＩＣカード１０が使用する秘密鍵を鍵変更コマンドが指定する秘密鍵に変更するＩＣカード１０を提供する。

【選択図】　　図２

特願２００３－０７１０３３

出　願　人　履　歴　情　報

識別番号　［０００００１００７］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社